REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-02-2005	FINAL	

4. TITLE AND SUBTITLE

Information Operation's Planners: Training and Education Without a Plan

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Jeremy R. Hill, USN

Paper Advisor (if Any): **N/A**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Combatant Commanders need a mix of Information Operations planners and capability specialists under their command to maintain the ability to dominate the full range of military operations. The difference between the two "types" of IO professionals should be based on their experience level. IO Planners must know extremely in-depth knowledge of the adversary, their psyche, network of connections, strengths, weaknesses, and ways of influencing each. Arguably, they are not alone in the planning cell and are supported by personnel from every office code within the command with additional possible support from inter-agency, coalition, and non-governmental organization representatives. The planners are expected to be able to articulate their intent, direction, restrictions, measures of effectiveness, and timeliness for the planning and employment of IO capabilities and related activities within their area of responsibility. In order to provide that understanding of the adversary, granularity and innovation in their plan, and ability to integrate their plan into the overall theater strategy or operation, their education and training levels need to meet a joint IO standard which has not been set by the Combatant Commanders. Professional Military Education must serve as a change agent for the military grappling with the information age. The educated force we develop and invest in today will significantly increase our chances of maintaining the information edge in the future.

15. SUBJECT TERMS

Information Operations, IO, Training, Combatant Commanders, Professional Military Education, Planners, Specialists, Professional Cadre, Core Capabilities

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		20	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

INFORMATION OPERATION'S PLANNERS: TRAINING AND EDUCATION WITHOUT A PLAN

By

Jeremy R. Hill
LCDR USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

10 February 2005

Abstract

Combatant Commanders need a mix of Information Operations planners and capability specialists under their command to maintain the ability to dominate the full range of military operations. The difference between the two "types" of IO professionals should be based on their experience level. IO Planners must know extremely in-depth knowledge of the adversary, their psyche, network of connections, strengths, weaknesses, and ways of influencing each. Arguably, they are not alone in the planning cell and are supported by personnel from every office code within the command with additional possible support from inter-agency, coalition, and non-governmental organization representatives. The planners are expected to be able to articulate their intent, direction, restrictions, measures of effectiveness, and timeliness for the planning and employment of IO capabilities and related activities within their area of responsibility. In order to provide that understanding of the adversary, granularity and innovation in their plan, and ability to integrate their plan into the overall theater strategy or operation, their education and training levels need to meet a joint IO standard which has not been set by the Combatant Commanders. Professional Military Education must serve as a change agent for the military grappling with the information age. The educated force we develop and invest in today will significantly increase our chances of maintaining the information edge in the future.

Table of Contents

INTRODUCTION

In May/June 1976, "the first known use of information warfare [by DoD] was in a briefing title and concept written by Dr. Tom Rona (then of Boeing) for Andrew Marshall."[1] DOD Directive TS3600.1 formally published the concept of information warfare for the Department of Defense in 1992. After years of strategic, operational, and tactical use and academic intellectual growth in the subject, the different military services diverged on how to organize, train, and equip their personnel to be able to conduct Information Operations (IO). In 1998, the U.S. Joint Chiefs of Staff signed the Joint Doctrine for Information Operations which required that the Combatant Commander's Information Operations staff must be able to do the following:

"…analyze the risk of compromise, adversary reprisal, collateral damage, escalation of hostilities, and uncoordinated or inadvertent counteraction of IO activities…"[2]

"…identify adversary vulnerabilities, devise required tasks and sub-tasks, and identify access opportunities and the means to exploit these vulnerabilities to achieve the JFC's objectives

…[identify] the adversary strategic and operational centers of gravity and [provide] guidance for defeating them

…[identify] and [provide] guidance on protecting the friendly centers of gravity and critical information infrastructures at the (Joint Force Commander) JFC operational level and at the strategic level"[3]

"...exploit, corrupt, disrupt, [degrade], or destruct adversary information systems and their will to fight (human element)"[4]

"…deny, disrupt, destroy, or otherwise control an adversary's use of information and information systems."[5]

Understand "…the biographical background of key adversary leaders, decision makers, communicators, and their advisors, to include motivating factors and leadership style."[6]

"…support forward presence operations, serve as a deterrent, provide general situational awareness, assist in the development of operational assessments and estimates, and support contingency operations."[7]

In 2003, Secretary of Defense, Donald H. Rumsfeld, published and distributed his *Information Operations Roadmap* which created another definition of IO. The difference

between this definition, and others, may not be significant but, it does obtain a bit more granularity than previous definitions.

> "The integrated employment of the core capabilities of Electronic Warfare [EW], Computer Network Operations [CNO], Psychological Operations [PSYOP], Military Deception [MILDEC] and Operations Security [OPSEC], in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own."[8]

The roadmap also identifies physical security, information assurance, counterintelligence, and physical attack as IO supporting capabilities and public affairs and civil-military operations as IO-related capabilities.

All of these requirements, and more, are expected from a staff that has a wide range of formal training and education, including no training at all up to specialty training, in a few of the core IO capabilities. The IO staff members are doing their professional best with the background education, training, experience, individual personality, and tenacious persistence to support the Combatant Commander in their mission and responsibilities-whether geographic or functional.

United States Code, Title 10, outlines that each service is required to organize, train, and equip their personnel. Combatant Commands must use the personnel and equipment presented by the services to accomplish the whole spectrum of peace and war in their geographic or functional areas of responsibility. Combatant Commanders need a mix of Information Operations planners and capability specialists[9] under their command to maintain the ability to dominate the full range of military operations. The difference between the two "types" of IO professionals should be based on their experience level. An IO planner should be an experienced capability specialist who has or is learning to integrate the various core IO capabilities.

COMBATANT COMMAND IO EXPERIENCE LEVELS

As stated by the Joint Staff J3, "Currently officers in important IO positions are often receiving their first exposure to IO."[10] Combatant Commander's IO staff members and IO Cells are expected to be able to articulate their intent, direction, restrictions, measures of effectiveness, and timeliness for the planning and employment of IO capabilities and related activities within their area of responsibility. In October 2003, the Secretary of Defense determined that the Department of Defense requires a cadre of IO professionals capable of planning and executing fully integrated IO which will support the Combatant Commanders. Unfortunately, the Combatant Commanders are not all created equal and do not all have the same needs. The five regional Combatant Commanders, U.S. Pacific Command (PACOM), U.S. European Command (EUCOM), U.S. Central Command (CENTCOM), U.S Southern Command (SOUTHCOM), and U.S. Northern Command (NORTHCOM), and the four functional Combatant Commanders, U.S. Joint Forces Command (JFCOM), U.S Strategic Command (STRATCOM), U.S. Transportation Command (TRANSCOM), and U.S. Special Operations Command (SOCOM) each have varying missions and responsibilities which may preclude a "cookie-cutter" set of IO planners and specialists though there should be an expected minimum of training for each type of billet.

The IO experience level at the combatant commands varies greatly. Some IO staffs may have several IO-experienced personnel, while others have none. It is not unusual to have an IO lead that has never had a previous IO-related job. The same is true for the IO staff. If the staffs have no experience with IO, their ability to execute well-constructed IO plans may be limited. When people come into the IO mission area with no IO experience, training must be rapid and comprehensive. The Joint Staff, along with the Combatant

Commanders, needs to determine the minimum training and education requirements for IO planners and specialists that will fill billets on the Combatant Command staffs.

INFLUENCING THE DECISION MAKER

The core of IO is to influence the decision maker, or makers, to do what you want them to do or think what you want them to think. Understanding the art and science of psychology is necessary to provide some context as to how to do this efficiently. PSYOP is not only a method of creating an influence on the decision maker it is also a system of reasoning for various methods used in an IO plan. According to Joint Publication 3-53, Psychological operations are defined as "planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[11] Often the role of PSYOP is thought of as leaflet drops, loud speaker announcements, radio broadcasts and, due to recent operations, electronic mail messages. These are methods of dissemination of psychological products and are only a small part of the process. It is a non-lethal way to multiply the effects of military capabilities through the direct communication of information to the enemy. The information operations, that are planned, must be developed and aimed at a well-defined target to reach a well-defined goal or objective through some transmission means and be able to provide some measure of effectiveness. PSYOP planners and specialists in the IO process are critical to the successful attainment of meeting these requirements. "It is essential that military PSYOP planners possess the ability to 'think outside the box,' because the ability to create and execute an effective PSYOP often depends upon the creativity used to develop and maintain a program. PSYOP planners must possess the following abilities:

-Understand each component's PSYOP and IO capabilities.
-Be intimately familiar with their command's assigned missions and operational area.
-Understand the concepts of centers of gravity, initiative, security, and surprise.
-Understand the psychological and cultural factors that might influence the adversary's planning and decision making.
-Understand potential adversaries' planning and decision-making processes (both formal and informal).
-Understand the specialized devices and weapons systems that are available to support PSYOP."[12]

The PSYOP planners and specialists require unique training to help them obtain the "traditional" and "out of the box" ideas and plans. Currently, there are six PSYOP courses taught throughout the Department of Defense. The maximum PSYOP course length is just over twelve weeks. The intent of PSYOP is to influence decision maker(s) behaviors that support the Combatant Commander's intentions at the strategic, operational, and tactical levels of warfare. Twelve weeks may give an individual an introduction in psychology but can not be considered adequate for someone to become a specialist. Psychology students must undergo four years (approx 120 quarter credit hours) of undergraduate studies to obtain a Bachelor of Arts in Psychology and an additional two to five years of masters (approx quarter 30-65 credit hours depending on college) and doctoral degree (approx 85-145 quarter credit hours depending on college). Though the PSYOP courses are relatively shorter in duration than a civilian doctorate program, it could be considered a good baseline for all service's IO specialists and planners to attend at least one of the DoD courses. The Department of Defense, and especially individual services, cannot afford to send all of their IO specialists and planners through six to eight years of education and training but, the difference in twelve weeks and six to eight years should demonstrate the need for a review of the process to consider an individual a specialist in psychological operations. This is especially true with the significant rise in costs for training, education, and personnel pay and

benefit costs each year, as well as a legally limited career of 36 years for those obtaining the most senior military ranks. Understanding the culture and preparation of the psychological or "soft" battlespace is necessary for the conduct of successful operations, especially, with the broad range of missions conducted by the U.S. military. Experienced and well-educated PSYOP and IO capability specialists and planners can be invaluable tools in these efforts. This is significant when one considers that if these types of measures are to be undertaken to influence the thinking and behavior of foreign leaders, it would require a level of understanding of a country's history, culture, politics, and mind-set at the very least, which is no easy task at the national, strategic, operational, tactical realms or in the academic world.

NO DEFINED JOINT IO EDUCATION AND TRAINING PLAN

Education without an adequate experience level can also lead to problems. The IO specialist and planners must obtain both as their careers progress.

> As quoted in the *The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy Quick Look Study* which was published in February 2004, "The GLOBAL GUARDIAN 04 After Action Report observed: The members of the IO Directorate possess varying degrees of experience in the five functional areas of the IO mission.…The workforce in the IO directorate is composed of individuals from various military occupation fields from the services. Although many have experience, training and education in related fields, such as intelligence, computer systems, missile or space operations, few have worked directly in one of the five designated mission areas of IO. While this is to be expected considering that none of the services have a formally defined career field for IO, as yet, the lack of a common understanding of Information Operations seems to impact the efficiency of accomplishing tasks to support ongoing operations. Watch standers spend much of their time researching answers to questions to which they should be able to respond based upon basic knowledge levels."[13]

Each service trains their IO professionals differently and currently not all services have created a separate IO career field. The Army has the Functional Area (FA) 30[14], the Air Force has the U-prefix[15], the Navy uses their Cryptology and Electronic Countermeasures

Officers[16], and the Marine Corps have created the Information Operations Officer (MOS 9634) and Information Operations Staff Officer (AMOS 9934)[17].

Each of these IO professional, or IO related career, classifications has different training requirements, expertise on systems, and measures of success. Since there are no integrated joint training and education requirements specifically for IO, the Combatant Commander and his staff can receive personnel with entirely different skill sets. A general requirement of Joint Professional Military Education (JPME) Phase I and Phase II is required. Depending on timing and availability, obtaining a graduate of JPME Phase II can be a challenge. Each Combatant Commander does have the ability to accept or deny the personnel nominated to come to their staff so they are able to influence the assignment and training process. The difficult part is in the formal training track while heading to the assignment and the various career timing aspects of the two individuals involved, the incumbent departing and the incoming relief. The Combatant Commanders need to insist that their personnel are trained at predetermined minimum joint IO standards and then insist that those personnel, who previously have been on a Combatant Command staff, return as they progress in their career. The requirement to complete one joint tour in the Combatant Commander IO division as a junior officer, a service-centered follow-on tour or two, and a return tour to the same, or even a different Combatant Commander IO division, as a more senior and/or experienced officer, would aid in the lack of continuity, education, training, and experience in these staffs.

The five core IO capabilities are not understood and applied the same way across the services. Instead, each service develops their own service-centric IO specialists to meet service specific needs because there are no specific joint Information Operations training requirements. In addition, development of EW, PSYOP and CNO specialists individually

could fulfill a career's worth of time without attempting to integrate a specialty in each of the areas. The training can not begin when an individual shows up at the staff. "There are significant differences in the capabilities of the IO staffs across the combatant commands. Two factors contribute to this condition. First, the experience and training levels of personnel arriving on the staff varies greatly. Some personnel are experts on a single discipline, PSYOP for example, but have little experience integrating. Others may have spent years doing IO. Second, combatant commands have several obstacles hindering their own training. Operational tempo (OPSTEMPO) demands often result in training and exercise opportunities being cancelled. OPSTEMPO may also prevent commands from sending their personnel to training courses."[18] The time available to conduct extensive training on the policies and doctrine of the Combatant Commander, regional requirements and intricacies, current stages of operations (peace and in crisis) throughout the area of responsibility, and Information Operations fundamentals are minimal due to the constant high level of ongoing operations. Even when there is no crisis in a Combatant Commander's area of responsibility, the IO plan and IO operations need to continue to promote peace, deter crisis, control crisis escalation, and even project power.

As an "IO capability specialist" becomes an expert in their specialty they also need to work on the integration of the other core capabilities. In order to learn how their specialty can be integrated they can either learn the other two remaining specialty areas, which can take years of training and experience, or they can move into the next role as IO planner. Currently, IO planners get basic instruction on how to employ IO tools and techniques, create and develop basic information operations and warfare plans and how to integrate IO plans into an overall joint force operational plan from school-house training. "Training for joint IO

planners presents a unique challenge because IO planners come from such a variety of ranks and experience. IO planners supporting exercises may range from the low enlisted ranks (e.g., E-2) through field-grade officers (O-5). Some may have experience in one or more IO functional areas such as electronic warfare or psychological operations, while others may have no prior IO-related experience…The three-week [Joint Information Operations Psychology Course] JIOPC, which is taught at both the [Joint Information Operations Center] JIOC and the [Joint Force's Staff College] JFSC, is the only source of formal IO planner training. The course is focused to support those going to joint IO staffs. Some JIOC team members who augment combatant command staffs say that the JIOPC is a good familiarization overview, but it is inadequate to provide all the specialized training required by the JIOC teams. Other concerns are that the course does not offer enough hands-on training and that it does not have enough capacity to handle everyone who needs to attend. Some of the planners who are not able to attend the JIOPC rely on Service-provided training or simply learn by on-the-job training."[19] Well-trained Joint IO planners are extremely critical to planning the information operations mission and integrating it into the overall Combatant Commander's theater and operation plans. The better the IO planner is trained and experienced, the more effective they will be able to perform the job.

COUNTERARGUMENTS

Up to this point in military operations, Combatant Commanders and their staffs have been able to conduct Information Operations despite this lack of formal training throughout their staff. They have been using information warfare and information-in-warfare tools since their inception. How can the previous arguments be valid and important to the Combatant Commander if they already have been and are conducting the IO missions and seem to be

fairly successful? As the U.S. moves toward more use of information warfare strategies, operations and tactics, so do its opponents. Several academic and IO experts say that the more the U.S. uses IO (particularly psychological and cyber-warfare) as a weapon, the more it exposes itself to IO by foreign governments, terrorist organizations, and even smaller entities such as an individual cyber-hacker. In comparison of conventional and nuclear weaponry, the U.S. remains the global leader of military power. The French have dubbed the U.S. as the sole "hyper-power" since the collapse of the former Soviet Union. With no legitimate single-nation contenders for the U.S. title of world superpower, it is not too much of a stretch of the imagination that a future adversary would seek out a non-traditional method of attacking perceived U.S. weaknesses.

> "One of the greatest potential threats to our national security is the prospect of 'information warfare' by foreign militaries against our critical infrastructures. We know that several foreign nations are already developing information warfare doctrine, programs, and capabilities for use against each other and the United States or other nations. Foreign nations are developing information warfare programs because they see that they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles Heel -- our reliance on information technology to control critical government and private sector systems. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. A serious challenge we face is even recognizing when a nation may be undertaking some form of information warfare. If another nation launched an information warfare attack against the United States, the [National Infrastructure Protection Center] NIPC would be responsible to gather information on the attack and work with the appropriate defense, intelligence, and national command authorities."[20]

Just as in all warfare communities, a continuous review of policies, doctrine, training and education are occurring. Information Operations is no different. It might be argued that IO methods, systems, and capabilities change relatively faster than the other warfare areas.

That rapidity of change makes it difficult to determine the best ways of training and educating an individual. The professional training and education pipeline can not be static. If the investment is made in an individual to become a specialist, or a planner, their skills can quickly become perishable if they are not kept up-to-date. In order to aid in proficiency, the Combatant Commander should insist that refresher training is conducted and that individuals, who were previously at one of the Unified Commands, return and continue to build their experience level to provide support for the theater operations. The current IO staff members at the various Combatant Commanders can not be considered lacking in individual skill areas. Each has some level of proficiency and training from their individual services which, in some cases, may be highly specific to the service-centric needs. This paper is not minimizing the hard work in recent and historic operations by these dedicated and extremely professional individuals in any way. The ubiquitous demand for information has shaped the current need of information specialists and planners capable of understanding the value of information in all of its roles: as knowledge, as target, as weapon. They might be able to provide the Combatant Commander with a more viable, and in some cases more innovative, approach to the various operations in the geographic or functional regions if they had a baseline of training which included psychological operations, information operations fundamentals and specialty courses in the regional or functional area they are going to be working in.

IO: SIGNIFICANT AT ALL LEVELS OF WARFARE AND POLICY

Information Operations represent a rapidly evolving and growing capability, as well as a problem, for Combatant Commanders and their IO staff members. The Combatant Commanders, like the rest of the world, are moving rapidly to take advantage of the new

opportunities presented by these changes. At the same time, current and potential U.S. adversaries (and allies) are also looking to exploit the evolving methods, hardware, and software and associated technologies for military purposes. As stated by President George Bush in the *National Security Strategy of the United States* (NSS), "The United States possesses unprecedented—and unequaled—strength and influence in the world. Sustained by faith in the principles of liberty, and the value of a free society, this position comes with unparalleled responsibilities, obligations, and opportunity. The great strength of this nation must be used to promote a balance of power that favors freedom."[21] The President also further states that IO must be used as a part of the strengths of the United States which he limits the use of IO to the military. The 2001 *Quadrennial Defense Review Report* pinpoints, or makes reference to, Information Operations/Warfare eighteen times and the *National Military Strategy of the United States of America 2004* ten times. Both documents also make several references to information-in-warfare and technology advances which enhance information-in-warfare capabilities. The importance in having a strong Information Operations Cell at the Operational level, i.e. the Unified Commands, is completely justified by the national and strategic embracement of the subject.

RECOMMENDATIONS

To conduct IO effectively is not an easy task and it is made even harder by not stressing that the joint force is educated at minimum levels of IO and the IO "specialists" and "planners" are educated and trained at a set level or standard. Once a Joint standard is set, the joint community, in concert with individual services, can work out who, what, where, when, and how long the courses should be to meet the needs of the joint force. Each Combatant Commander IO Staff lead, and their staff, should take a independent look at what

is the ideal mix of IO specialists and planners required to ensure the appropriate goals of training, education, and experience are meshed together with learning from the past, working in the current operations, and be able to plan for future operations. IO is a continuous operation in all areas of the Combatant Commander's functional or geographic region. The specialists and planners need to have a basic level of expertise in the various pillars of IO in order to be able to provide the Commander a credible IO plan. It is difficult to think "outside of the box," or innovatively, if you don't even know what is "inside the box."

An IO planner should be an experienced capability specialist who has learned, or is learning, to integrate the various core IO capabilities. The Department of Defense, and especially individual services, cannot afford to send all of their IO specialists and planners through six to eight years of education and training but all should be required to go through an intense education regimen where learning psychology basics and decision maker influence are the primary concepts. Finally, in order to aid in proficiency, the Combatant Commander should insist that individuals, who were previously assigned to one of the Unified Commands, be reassigned to a Unified Command later in their career and get refresher training enroute to build their experience level and provide support for the theater operations.

CONCLUSION

The beginning of this document listed a non-exhaustive set of requirements that the Information Operations planners must be able to accomplish while assigned to a Combatant Commander's staff. The list ranges from knowing extremely in-depth knowledge of the adversary, their psyche, network of connections, strengths, weaknesses, and ways of influencing each. Arguably, they are not alone in the planning cell and are supported by

personnel from every office code within the command with additional possible support from inter-agency, coalition, and non-governmental organization representatives. The planners are expected to be able to articulate their intent, direction, restrictions, measures of effectiveness, and timeliness for the planning and employment of IO capabilities and related activities within their area of responsibility. In order to provide that understanding of the adversary, granularity and innovation in their plan, and ability to integrate their plan into the overall theater strategy or operation, their education and training levels need to meet a joint IO standard which has not currently been set by the Combatant Commanders. Professional Military Education (PME) must serve as a change agent for the military grappling with the information age. Raising awareness of the threat, opportunities, and vulnerabilities inherent in the changes underway can best be done through the PME structure. The joint IO standard needs to be go beyond the basic joint force requirements of JPME Phases I and II and may even need to compensate for individual service differences in training and education of their IO professional cadre. The educated force we develop and invest in today will significantly increase our chances of maintaining the information edge in the future.

NOTES

[1] Joint Command Control and Information Warfare Staff, Information Operations: The Hard Reality of Soft Power, (Norfolk, VA: National Defense University, 2002), 129.

[2] Ibid, V-1.

[3] Ibid, V-3.

[4] Ibid, II-9.

[5] Ibid, II-11.

[6] Ibid, II-13.

[7] Ibid, II-11.

[8] Department of Defense, Information Operations Roadmap, (Washington, DC: 30 October 2003), 11.

[9] "IO capability specialists are functional experts in one or more of the highly specialized capabilities of CNO, EW, or PSYOP." Department of Defense, Information Operations Roadmap, (Washington, DC: 30 October 2003), 34.

[10] Smith, Jim, "Developing Information Operations IO Warriors," JPME Prospective Research Topics Database (PRTD), <http://jdeis.cornerstoneindustry.com/jdeis/eduResearch/users/topic.jsp?searchTerm_inform>, [05 Dec 2004.]

[11] Joint Chiefs of Staff, Doctrine for Joint Psychological Operations, Joint Pub 3-53, (Washington, DC: 5 Sept 2003), IX.

[12] Army Department, Psychological Operations, FM 3-50.30, (Washington, DC: June 2000), 7-34.

[13] U.S. Strategic Command Global Guardian (GG 04) Final Exercise Report, IATAC, Information Assurance Technology Analysis Center, 3190 Fairview Park Drive, Falls Church, VA 22042, Contract Number SPO 700-98-D-4002, TAT 03-21, DO 192, 21-31 October 2003 page A-11 as quoted in. DiGiovanni, Frank, The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy Quick Look Study, SPO 700-98-D-4002, (Falls Church, VA: IATAC, February 2004), 27.

[14] Additional information can be at: U.S. Army Human Resources Command, "Purpose of Information Operations Career Field (IOCF)", 10 August 2004, <https://www.perscomonline.army.mil/opfamio/default.htm>, [17 January 2004] and Army Department, Commissioned Officer Development and Career Management, Department of the Army Pamphlet 600–3, (Washington, DC: 1 October 1998) 226.

[15] Additional information can be found at: Air Force Department, Officer Classification, Air Force Manual 36-2105, (Washington, DC: 31 October 2004), 43.

[16] Additional information can be found at: Bureau of Naval Personnel, Cryptology in the Navy "Overview", 06 December 2001, <http://www.bupers.navy.mil/pers4410/overview.html>, [17 January 2004].

[17] Additional information can be found at: PP&O, Information Operations and Space Integration Branch, also referred to as PLI, established an additional MOS, Information Operations staff officer (AMOS 9934) which was published with "Information Operations Career Force and Space Cadre," MARADMIN 273/03, DTG: 111200Z JUN 03 and Navy Department, U.S. Marine Corps, Military Occupational Specialties Manual, Marine Corps Order P1200.7Z, (Washington, DC: 27 April 2004), 1-109,1-110,1-145.

[18] DiGiovanni, Frank, The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy Quick Look Study, SPO 700-98-D-4002, (Falls Church, VA: IATAC, February 2004), 34.

[19] Ibid, 35.

[20] Freeh, Louis J, "Statement," Director, FBI, Cybercrime, Before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies, 16 February, 2000.

[21] President, The National Security Strategy of the United States of America, (Washington, DC: September 2002), 1.

BIBLIOGRAPHY

Alberts, David S. The Unintended Consequences of Information Age Technologies. Washington, DC: National Defense University Press. April 1996.

Berkowitz, Bruce D. The New Face of War: How War Will Be Fought in the 21st Century. New York: The Free Press. 2003.

Bloom, Bradley. "Information operations in support of special operations." Military Review (January-February 2004). 26 December 2004. <http://www.findarticles.com/p/articles/mi_m0PBZ/is_1_84/ai_n6112513> [26 December 2004].

Bowdish, Randall, G. "Information Age Psychological Operations". Military Review (December 1998-February 1999). 28-36.

Bureau of Naval Personnel. Cryptology in the Navy. "Overview". 06 December 2001. <http://www.bupers.navy.mil/pers4410/overview.html>. [17 January 2004].

Defense Science Board Task Force. The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict. Washington, DC, DSB, May 2000.

Department of Defense. Information Operations Roadmap. Washington, DC: 30 October 2003.

_____. Information Operations (Draft). Department of Defense Directive 3600.1. Washington, DC: 17 May 2004.

DiGiovanni, Frank. The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy Quick Look Study. SPO 700-98-D-4002. Falls Church, VA: IATAC, February 2004.

Emory, Norman. "Information Operations in Iraq." Military Review (May-June 2004). 11-14.

Gillam, Mary M. Information Warfare: Combating the Threat in the 21st Century. Maxwell AFB, AL: Air Command and Staff College. March 1997.

Haeni, Reto E. Information Warfare an Introduction. Washington, DC: George Washington University Cyberspace Policy Institute. January 1997.

Haugrud, Anthony, Gary C. Lehmann, and Curtis Phillips. "Rethinking Joint Training." Joint Force Quarterly. (Winter 2000-1). 66-70.

Joint Command Control and Information Warfare Staff, ed. Information Operations: The Hard Reality of Soft Power. Washington, DC: National Defense University Press, 2002.

_____. Joint Information Operations Planning Handbook. Washington, DC: National Defense University Press, July 2002.

Kuehl, Daniel. "Joint Information Warfare". An Information-Age Paradigm for Jointness. 30 January 2005. <http://www.ndu.edu/inss/strforum/SF105/forum105.html>. [30 January 2005].

Lord, Carnes and Frank R. Barnett, ed. Political Warfare and Psychological Operations Rethinking the US Approach. Washington, DC: National Defense University Press. 1989.

Lungu, Angela Maria. War.Com: The Internet and Psychological Operations. Newport, RI: U.S. Naval War College, 5 February 2001.

Molander, Roger C., Andrew S. Riddile and Peter A. Wilson. Strategic Information Warfare A New Face of War. Santa Montica, CA: RAND. 1996.

Rhodes, J.E. A Concept for Information Operations. Quantico, VA: Marine Corps Combat Development Command. 15 May 1998.

Smith, Jim. "Developing Information Operations IO Warriors." JPME Prospective Research Topics Database (PRTD). <http://jdeis.cornerstoneindustry.com/jdeis/eduResearch/users/topic.jsp?search Term_inform>. [05 Dec 2004].

Tangredi, Sam J. ed. Globalization and Maritime Power. Washington, DC: National Defense University Press. December 2002.

U.S. Air Force Department. Officer Classification. Air Force Manual 36-2105. Washington, DC: 31 October 2004.

_____. Information Operations. Air Force Doctrine Document 2-5. Washington, DC: 04 January 2002.

U.S. Army Department. Information Operations: Doctrine, Tactics, Techniques, and Procedures. FM 3-13. Washington, DC: November 2003.

_____. Psychological Operations. FM 3-50.30. Washington, DC: June 2000.

_____. Staff Organization and Operations. FM 101-5. Washington, DC: 31 May 1997.

_____. Tactics, Techniques, and Procedures for The Targeting Process. FM 6-20-10. Washington, DC: 8 May 1996.

_____. Commissioned Officer Development and Career Management. Department of the Army Pamphlet 600–3. Washington, DC: 1 October 1998.

U.S. Army Human Resources Command. "Purpose of Information Operations Career Field (IOCF)". 10 August 2004. <https://www.perscomonline.army.mil/opfamio/default.htm>. [17 January 2004].

U.S. Congress. Senate. Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies. Cybercrime, Hearings before the Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies, 16 February, 2000.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, DC: 1 February 1995.

_____. Joint Doctrine for Military Operations Other Than War. Joint Pub 3-07. Washington, DC: 16 June 1995.

_____. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: 9 October 1998.

_____. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington, DC: 7 February 1996.

_____. Doctrine for Joint Psychological Operations. Joint Pub 3-53. Washington, DC: 5 Sept 2003.

_____. Joint Doctrine for Targeting. Joint Pub 3-60. Washington, DC: 17 January 2002.

_____. Joint Doctrine for Campaign Planning. Joint Pub 5-00.1. Washington, DC: 25 January 2002.

_____. Joint Vision 2020. Washington, DC: June 2000.

_____. Joint Training Policy and Guidance for the Armed Forces of the United States (Draft). CJCSI 3500.01C. Washington, DC: 31 July 2004.

_____, Officer Professional Military Education Policy. CJCSI 1800.01B. Washington, DC: 30 August 2004.

U.S. Marine Corps Intelligence Activity. Information Operations/Information Warfare Generic Intelligence Requirements Handbook. MCIA-2700-001-03. Quantico, VA: Marine Corps Intelligence Activity: November 2002.

U.S. Naval Postgraduate School. Information Systems and Operations Curriculum 356. 30 January 2005. <http://www.iso.nps.navy.mil/index.htm>. [30 January 2005].

U.S. Navy Department. Psychological Operations. OPNAVINST 3434.1. Washington, DC: 22 Dec 1997.

U.S. Navy Department. U.S. Marine Corps. Marine Corps Planning Process. MCWP 5-1. Washington, DC: 24 September 2001.

_____."Information Operations Career Force and Space Cadre". MARADMIN 273/03. DTG: 111200Z JUN 03.

_____. Military Occupational Specialties Manual. Marine Corps Order P1200.7Z. Washington, DC: 27 April 2004.

U.S. President, The National Security Strategy of the United States of America. Washington, DC: September 2002.

Whitley, Gary L. PSYOP Operations in the 21st Century. Carlisle, PA: U.S. Army War College. 10 April 2000.